国連サイバー犯罪条約——審議が大詰めにはいった世界規模の監視国際法

JCA-NET セミナー

2024 年 8 月 25 日

(2024 年 9 月 9 日改訂)

小倉利丸

toshi@jca.apc.org

国連サイバー犯罪条約——審議が大詰めにはいった世界規模の監視国際法

このセミナーで昨年９月に、国連サイバー犯罪条約をとりあげて１年になります。

今年９月にはこの条約案が国連総会にかけられる可能性がでてきています。この条約は、「サイバー犯罪」の取り締まりを名目にしていますが、実際の条文案では、コンピュータを用いた違法行為を広範囲にわたって対象としており、各国の捜査機関が国境を超えた連携をとりながら、私たちのパソコンやスマートフォンなどへの監視や捜索をより広範囲にわたり、より強力に行なえるような内容になっています。もしこの条約が成立し、日本が批准することになれば、既存の刑事司法制度を根底から覆しかねない大きな影響を及ぼすことになります。

この条約は、ロシアなどが提案し、これに日頃は対立関係にある欧米や日本などが相乗りして制定への作業が進められてきたという経緯をもっています。また、この条約策定は、各国の警察などが中心となり国連の麻薬犯罪事務所（UNOÐC）が事務局となって推進してきたもので、人権を脆弱にしかねないと国連の人権機関から危惧されていきたものでもあります。

特に人権団体などが注視しているのは、抑圧的な政策をとる国々が、この条約を利用して、自国の反政府運動やジャーナリストへの弾圧の手段に用いたり、難民やLGBTQなど権利の脆弱な人々への悪影響、令状主義の形骸化や警察の国境を超えた連携強化が問題視されています。このセミナーでは前回に引き続き条約草案について、最新の状況を紹介するとともに、人権団体などが条約案の何を問題としているのかについても紹介します。

国連サイバー犯罪条約——審議が大詰めにはいった世界規模の監視国際法

資料 国連サイバー犯罪条約日本語粗訳 https://cryptpad.fr/pad/#/2/pad/view/mCpXUk3p1vOTwd+IkxEVwEjD5K17IL2oX2qGxVtP3sk/

(2023年9月のセミナー)国連サイバー犯罪条約―今争点となっている深刻な課題とは https://pilot.jca.apc.org/nextcloud/index.php/s/GqBN8EDJABDR7ak

国連サイバー犯罪条約関連のドキュメント https://www.jca.apc.org/jca-net/ja/node/374

(EFF)国連サイバー犯罪条約年表 https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/eff_un-cybercrime-treaty-timelinemain-content_jp/

(EFF)国連サイバー犯罪条約草案は、プライバシーやデータ保護に関する強固 なセーフガードなしに国家の監視権限を危険なまでに拡大する https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/eff_un-cybercrime-draft-convention-dangerously-expands-state-surveillance-powers_jp/

(EFF)セキュリティ研究者とジャーナリストを危険にさらす：国連サイバー犯 罪条約案を非難すべき理由 https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/eff_journalists-and-security-researchers-risk-why-you-should-hate-proposed-un_jp/

(EFF)国連監視条約草案の危険な欠陥に対処するよう、国連の主要人権担当官、 企業、技術団体から要請が相次ぐ https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/eff_calls-mount-principal-un-human-rights-official-business-and-tech-groups-address_jp/ (EFF)広範な適用範囲は、表現行為に対する国境を越えたスパイ行為を容認す る：

国連サイバー犯罪条約草案に反対すべき理由 https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/eff_overbroad-scope-will-authorize-cross-border-spying-acts-expression-why-you-should_jp/

国連サイバー犯罪条約――審議が大詰めにはいった世界規模の監視国際法

最近の報道

(読売 8/10) 国連総会で「サイバー犯罪条約」採択へ…ロシアが主導、政府監視に懸念

条約はロシアが主導した。強権国家が反体制派の監視を目的として条約を悪用するのではないかとの懸念が米欧では出ている。日本は今後、条約内容を精査し、署名と批准の是非を検討する。

条約はネット上の不正アクセスや児童ポルノ拡散などの犯罪捜査で国際協力のあり方を定めたほか、途上国に対するネット犯罪の取り締まりに向けた技術支援が盛り込まれている。

もともと２００１年に欧州評議会が別のサイバー犯罪条約を採択し、日米など７５か国が批准しているが、未批准のロシアが「西側諸国による不完全なものだ」(国連外交筋) として包括的な新条約が必要だと主張し、２２年に交渉が始まった。米欧は採択の前提として、「表現の自由」の抑圧や差別につながる捜査について、協力要請を拒否できる条項を明記するよう要求。当初、ロシアや中国は反発したが、最終的に盛り込まれた。

(共同→東京 8/9) 国連、サイバー犯罪条約を採択「国家による監視」に懸念も

不正アクセスや児童ポルノ流布などの犯罪を取り締まるためのサイバー犯罪条約が８日、ニューヨークの国連本部で開かれた条約制定交渉会合で、議場の総意により無投票で採択された。ロシアが主導した。国際的なサイバー犯罪捜査に役立つことが期待されるが、人権団体などからは「国家による監視や弾圧につながる」と懸念が強まっている。日本や欧米が中心となり、２００１年にハンガリー・ブダペストで署名されたインターネット犯罪撲滅を目指した同種の条約がすでに発効しているが、ロシアは地域条約に過ぎないとして、国連を通した条約制定を推進していた。近く国連総会でも正式に採択される見通し。

国連サイバー犯罪条約——審議が大詰めにはいった世界規模の監視国際法

最近の報道

(NHK 8/9) 国境越えたサイバー犯罪取り締まる 新国際条約草案 国連で合意

国連のサイバー犯罪条約は、ネット詐欺や資金洗浄、児童ポルノの拡散など、インターネットで国境を越えて行われる犯罪の取り締まりを強化するため、国連総会での決議を受けて議論が進められてきたもので、８日、委員会で草案が合意されました。

条約は「サイバー犯罪に関わる者たちの安住の地を無くす」ことを掲げ、締約国に取り締まりに向けた対策の強化を義務づけています。

また条文では、サイバー犯罪の被害が拡大している途上国への技術支援など、国際協力も促進するとしていて、来月の国連総会で正式に採択される見通しです。

条約の草案づくりにあたっては、ロシアや途上国が積極的だった一方で、欧米諸国の間では「表現の自由」の制限や国家による監視の強化につながるおそれがあるとして人権への影響を懸念する声もあり、議論が難航していました。

委員会の副議長として議論のとりまとめにあたってきた外務省の割澤広一国際安全・治安対策協力室長は「日本としては、人権の保障と犯罪への対処が両立できるよう交渉に取り組んできた。国際社会が国境をまたいで行われるサイバー犯罪にしっかり対処できる環境が整ったのは大きな一歩だ」と話し、条約の意義を強調していました。

経緯

- 2017年10月

  ロシア連邦は、加盟国への配布を目的とした「サイバー犯罪との闘いにおける協力に関する国連条約 the United Nations Convention on Cooperation in Combating Cybercrime」の草案を含む書簡を国連総会に提出する。

- 2019年11月

  ベラルーシ、カンボジア、中国、イラン、ミャンマー、ニカラグア、シリア、ベネズエラとともにロシアが提唱した、サイバー犯罪と闘うための国際条約を制定する決議案が国連総会で可決(賛成79反対60棄権33)される。この決議には、アメリカ、EU、日本その他の国々が 反対した。進歩的コミュニケーション協会やEFFなどの人権団体は、「人権の行使や社会的・経済的発展を促進するためのインターネットの利用を損なう恐れがある」との懸念を理由に、総会で決議案に反対票を投じるよう強く求めた。(国連資料)

- 2019年12月

  国連総会は、「犯罪目的の情報通信テクノロジーの使用に対抗することに関する」国連条約を起草するための 特別委員会(AHC)を設置する決議を採択する。以後反対した各国が条約制定を肯定的に捉えて関与するようになる。

- 2021年5月

  AHCが設立総会を開き、 160カ国以上の 代表が交渉の概要と方法に合意する。 AHCは、 2022年から少なくとも6回開催。

経緯

- 2022年2月

  AHCの最初の公式会合がニューヨークで10日間 開かれ、交渉が始まる。

  第1回会合に提出された加盟国の意見を見ると、何が「サイバー犯罪」を構成するのか、条約はどの程度拡大されるのかについて、コンセンサスを明確に欠いていることがわかる。ブラジル、 ドミニカ共和国、 欧州連合（EU）、リヒテンシュタイン、 ノルウェー、 スイス、 英国、 米国などの国々は、犯罪に関連する焦点を絞ることを主張し、この条約がインターネットに広範な管理を課すために使用されることを警告している。また、テロ扇動（中国、ロシア）、偽情報（中国、インドネシア）、著作権侵害（インドネシア、リヒテンシュタイン、メキシコ、ノルウェー、ロシア、米国）など、コンテンツ関連の犯罪を含めるよう求める国もある。

- 22024年7月から8月

  最終交渉会議7月31日から8月9日までニューヨークで開催

- 2024年9月

  第79回国連総会（ UNGA 79 ）は2024年9月10日（火）。国連サイバー犯罪条約の最終草案が総会に提出され、セッション中に審議

サイバー犯罪の定義とは…

サイバー犯罪やサイバー攻撃の国際的な定義はない。

国連薬物犯罪事務所(UNODC　サイバー犯罪条約の事務局)の説明や先行するブダペスト条約などから、以下のように分類できる

(a) 情報通信テクノロジーを標的にした犯罪。マルウェアの作成、拡散、配備、ランサムウェアデータ過負荷によるウェブサイトのオフライン化(DDOS 攻撃)など。

(b) 情報通信テクノロジーを手段とした犯罪。オンライン詐欺、オンライン薬物購入、オンライン・マネーロンダリング、インフラへのネットワークを介した攻撃など。

個別の事案として

(c) 子どもの性的搾取と虐待。インターネット上の虐待、ダークネット・フォーラム、そして最近では「 sextortion 」として知られる恐喝による自作画像の搾取など。

(d)　著作権関連の犯罪。

(a) より (b) の方が大幅に「サイバー犯罪」に含まれる行為が拡大される。 (c)(d) は監視社会化を正当化する手段として利用されやすい。

日本の態度

外務省の定義

「不正アクセスやランサムウェアなどコンピュータ・システムを攻撃するような犯罪及びコンピュータ・システムを利用して行われる犯罪」

(https://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/index.html)

警察庁警察白書の定義

「不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪その他犯罪の実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪」(2024年p.112)

(https://www.npa.go.jp/hakusyo/r06/pdf/06_dai3sho.pdf)

いずれもICTを手段とした違法行為であれば「サイバー犯罪」のカテゴリーに入れており、またいわゆる「児童ポルノ」も含まれており、非常に幅が広い。

日本の態度

既存の国際条約について。

日本はブタペスト条約を批准している。外務省のウエッブから。

□サイバー犯罪に対処するための法的拘束力のある国際文書の作成が必要であるとの認識が欧州評議会において共有されるようになり、平成 9 年（ 1997 年) 以降、欧州評議会におけるサイバー犯罪を取り扱う専門家会合においてサイバー犯罪に関する条約の作成作業が行われてきました。その結果、平成 13 年（ 2001 年 ）9 月に行われた欧州評議会閣僚委員会代理会合においてこの条約の案文について合意し、同年 11 月 8 日に行われた欧州評議会閣僚委員会会合において正式に採択されました。その後、同条約は、平成 16 年（ 2004 年 ）7 月に発効しています。

□同条約は、サイバー犯罪から社会を保護することを目的として、コンピュータ・システムに対する違法なアクセス等一定の行為の犯罪化、コンピュータ・データの迅速な保全等に係る刑事手続の整備、犯罪人引渡し等に関する国際協力等につき規定しています。

□我が国は、平成 24 年（ 2012 年 ）7 月 3 日に同条約の受諾書を欧州評議会（ストラスブール) の事務局長に寄託しました。これにより、同条約は、我が国については平成 24 年（ 2012 年 ）11 月 1 日に効力が発生しました。

サイバー犯罪に関する条約 (和文テキスト・条約説明書)

欧州評議会 (CoE) のウェブサイト（サイバー犯罪に関する条約 ）（英語 ）

日本の態度

既存の国際条約について。

・サイバー犯罪に関する条約の第二追加議定書

・平成29年（2017年）以降、欧州評議会において、容易に国境を越えるサイバー犯罪対策のための枠組みとして、他の締約国から、より迅速かつ円滑な手続による電子的形態の証拠の収集を可能にすること等を目的として、サイバー犯罪に関する条約の追加議定書の作成交渉が行われました。そして、令和3年（2021年）11月17日の欧州評議会閣僚委員会において、「協力及び電子的証拠の開示の強化に関するサイバー犯罪に関する条約の第二追加議定書」が採択されました。

・我が国は、令和5年（2023年）8月10日に同議定書の受諾書を欧州評議会（ストラスブール）の事務局長に寄託しました。

・同議定書は、サイバー犯罪に関する条約の締約国のうち5か国が同議定書に拘束されることに同意する旨を表明した日の3か月後の月の翌月の初日に効力を生じます。（令和6年（2024年）8月現在、その旨を表明した締約国は我が国を含め2か国にとどまり、現時点で未発効です。）

協力及び電子的証拠の開示の強化に関するサイバー犯罪に関する条約の第二追加議定書

欧州評議会（CoE）のウェブサイト（サイバー犯罪に関する条約の第二追加議定書）（英語）

日本の態度

外務省などのウエッブ上での公開情報（日本語）はほとんどみあたらないようだ。日本がどのような態度をとってきたのかを全体として把握することは難しいが、反対しない可能性が高い。日本は、日米同盟とロシアや中国との対立関係という地政学的な思惑で慎重審議を求めているが、人権への関心は高くない。

これまでに日本が国連に提出した文書として以下がある。（これ以外にもあるかもしれない）

2020年8月会合に向けて

https://cryptpad.fr/pad/#/2/pad/view/bzqDCo0Tcx3ET4Qw33ANYMt3-jFf0JcBQFXvpR1dspw/

2021年10月29日

https://cryptpad.fr/pad/#/2/pad/view/vDolbcjL-kbAtXuEQDVis9zB8B65395OrX3nW6rUDvw/

2022年4月8日

犯罪化、一般規定、および
手続き措置と法執行に関する寄稿 https://cryptpad.fr/pad/#/2/pad/view/cfnTyCRi7XKqEhWw+boHIJSVbMuoEoAcSMHdK5I0uNs/

権威主義国家であれ民主主義国家であれ警察権力は人権と相容れない

- 人権より国益を重視する流れが国連の過半数を占めている
- 人権を重視する諸国も、国内の人権団体などによる働きかけの影響が大きい
- 総じて人権団体の弱体な国ほど人権への関心が低く、警察などの影響力が大きくなる
- UNODC は警察官僚の影響力が強い国連の組織であり、人権組織とは性格が異なる。事実、国連人権高等弁務官事務所はこの条約案を厳しく批判してきた
- 日本の現状はとうてい人権を重視しているとはいえない。とくに日本の司法警察の制度は人質司法、令状主義の形骸化、構造的な民族差別意識、警備公安警察の肥大化や死刑制度への固執など国際的にみても民主主義国家とはいいがたい性格が色濃い

条約とは

憲法上条約の締結は内閣の事務であり、国会の承認が必要。

いったん締結した条約は遵守義務を負う

第73条　内閣は、他の一般行政事務の外、左の事務を行ふ。

　三　条約を締結すること。但し、事前に、時宜によつては事後に、国会の承認を経ることを必要とする。

第98条　この憲法は、国の最高法規であつて、その条規に反する法律、命令、詔勅及び国務に関するその他の行為の全部又は一部は、その効力を有しない。

　2　日本国が締結した条約及び確立された国際法規は、これを誠実に遵守することを必要とする。

言うまでもなく、憲法に違反する条約の締結はできないはずだが、現実には違憲といえる条約の締結がなされている。（例えば9条に抵触する日米安保条約など）

条約とは

国連サイバー犯罪条約と憲法との関連

第 21 条 集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。

２ 検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

第 35 条 何人も、その住居、書類及び所持品について、侵入、捜索及び押収を受けることのない権利は、第 33 条の場合を除いては、正当な理由に基いて発せられ、且つ捜索する場所及び押収する物を明示する令状がなければ、侵されない。

２ 捜索又は押収は、権限を有する司法官憲が発する各別の令状により、これを行ふ。

国連サイバー犯罪条約の基本的性格

条約の名称　**「国連サイバー犯罪条約――情報通信テクノロジーシステムを利用して行われる特定の犯罪と闘い、重大犯罪の電子的形態の証拠を共有するための国際協力を強化」**

この条約の基本的な性格は違憲であり、日本はこの条約を締結すべきではない。内閣は締結の手続きをとることは憲法に反する行政権の行使である。

- 通信ネットワークを監視することや、通信内容を国家が密かに把握することは、21条に違反する行為
- 裁判所の令状なしでのネットットの捜索などは31条に違反する行為

国連サイバー犯罪条約の基本的な性格は、ネットワークを監視し、通信の内容を取得すること、裁判所のチェックなしの捜査機関による権限強化により各国の捜査機関が迅速に行なえるように、国内法を改悪するように強制するところにある。

国連サイバー犯罪条約への批判

電子フロンティア財団の批判から

提案されている国連サイバー犯罪条約は、広範な監視条約であり、国内に侵入的な監視措置を課し、国家間の監視とデータ共有における協力を義務づけている。この条約には法的相互援助の規定があり、サイバー犯罪に関連する捜査や訴追において国家が相互に援助することを要件としている。また、重大とみなされる犯罪であれば、電子的証拠の収集、入手、保全、共有が認められており、人権保障措置はほとんどない。この協力は、人権に関する実績が乏しい国々にも及ぶ。この条約案の交渉は、ロシア連邦からの物議を醸す提案によって2022年に始まった。

もしこの条約案が採択されれば、世界中の監視法が書き換えられることになる。人権擁護活動家、ジャーナリスト、権力に真実を語る人々など、政府によってしばしば標的にされる人々を含む何百万もの人々が影響を受けることになる。義務的で、明確で、強制力のあるセーフガードがなければ、この条約案は人権の保護というよりも、国家の乱用や国境を越えた抑圧の道具となるリスクがある。

国連サイバー犯罪条約への批判

電子フロンティア財団の批判から (続き 1)

条約草案のタイトルは誤解を招き、問題がある。 サイバー犯罪を ICT を通じて行われるあらゆる犯罪と同一視することは、概念的にも実際的にも有害である。サイバー犯罪は、コンピュータ・システム、ネットワーク、データに対する行為に焦点を当てるべきである。その定義を広げようとする最近の動きは、表現や人権を犯罪化することにつながっている。

不十分な人権保護措置。 効果的な人権保護には、監視を実施する前の司法の承認、実施された措置の透明性、捜査を危うくしない限りデータのアクセス時にユーザーに通知することなどが要件になるが、こうした保護措置が省かれている。この条約は、既存の強固な人権基準を損なう可能性がある。

強固な保護措置のない、極めて侵入的な秘密スパイ権限。 草案は、広範な秘密の監視を認めており、国内的にも国際的にも重大なリスクをもたらしている。この草案では、非サイバー犯罪や、ある国では合法だが他の国では犯罪とされる活動を含む幅広い犯罪について、トラフィックデータやコンテンツのリアルタイム傍受を認めている。サービスプロバイダーは秘密裏に協力せざるを得ず公的チェックが効かない。スパイ活動や証拠収集における国境を越えた援助の濫用の可能性を大幅に増大させ、国境を越えた弾圧や人権侵害のリスクを悪化させる。

国連サイバー犯罪条約への批判

電子フロンティア財団の批判から (続き 2)

国際協力の章の広範な範囲は、依然として深刻な脅威である。条約草案では、ある国では重罪とされながら、ある国では合法とされている活動について、ある国が他国をスパイ活動で支援することを認めている。

LGBTQ とジェンダーの権利に対するリスク。条約の広範な適用範囲は、LGBTQ+ とジェンダーの権利に重大なリスクをもたらす。特に国内法がこれらの表現を重大な犯罪として犯罪化した場合、性別や性的指向に基づいて個人を標的にするために悪用される可能性がある。これは、社会から疎外された集団を迫害するためにサイバー犯罪法が悪用された歴史を考えれば、特に懸念すべきことである。

強制的な技術支援。草案では、当局は特定のコンピュータやデバイスを熟知している者に対し、ユーザー ID や個人データ、位置情報などを含む情報へのアクセスに必要な情報を提供するよう強制できる法律を各国に求めている。

国連サイバー犯罪条約への批判

電子フロンティア財団の批判から (続き 3)

広範な範囲と過剰な犯罪化のリスク。 条約草案には、「グルーミング」や CSAM(子どもの性的搾取関連の資料) など、サイバー犯罪だけでなく幅広い犯罪が引き続き含まれている。条約の範囲を不必要に拡大し続け、表現や集会を含む合法的なオンライン活動を過度に犯罪化するリスクをはらんでいる。

セキュリティ・リサーチやその他の公益活動に対する保護が不十分である。 条約案は、セキュリティリサーチ、ジャーナリズム、内部告発を犯罪化の対象から除外しておらず、世界的にサイバーセキュリティと報道の自由に重大なリスクをもたらす。

最終草案の内容

構成

前文

第一章 一般規定

第 1 条 目的

第 2 条 用語の用法

第 3 条 適用範囲

第 4 条 他の国際連合条約及び議定書に従って定められた犯罪

第 5 条 主権の保護 [暫定的合意]

第 6 条 人権の尊重 人権の尊重

第二章 刑事罰

第 7 条 不正アクセス

第 8 条 違法傍受 [暫定的合意]

第 9 条 電子データへの妨害行為 Interference

第 10 条 情報通信テクノロジー・システムの妨害 [暫定的合意]

第 11 条 デバイスの不正使用 [暫定的合意]

第 12 条 情報通信技術システム関連偽造

最終草案の内容

構成（続き）

第 13 条． 情報通信テクノロジーシステムに関連する窃盗又は詐欺

第 14 条：オンライン上の子どもの性的虐待に関する犯罪 オンラインにおける子どもの性的虐待または子どもの性的搾取に関する犯罪

第 15 条 子どもに対する性犯罪を目的とする勧誘またはグルーミング［暫定的合意］

第 16 条 親密な画像の同意のない流布

第 17 条 犯罪収益の洗浄 ［暫定的合意］

第 18 条 法人責任［暫定的合意］

第 19 条 参加及び企て［暫定的合意］

第 20 条 時効の定め［暫定的合意］

第 21 条 訴追、判決 adjudication 及び制裁［暫定的合意］

第三章 管轄権

第 22 条 管轄権

第四章 手続き上の措置および法の執行

第 23 条 手続的措置の範囲

第 24 条 条件及び保障

第 25 条 保存された電子データの迅速な保全 preservation［暫定的合意］

捜査機関の権限などを規定しているが、これが第 2 章の犯罪に限定した措置であるという明言がないので、あらゆる犯罪捜査などに適用できる？

最終草案の内容

随所に「迅速な」という文言が。これは裁判所の許可などの手続きを経ないで捜査機関単独の判断で行なえることを意図しているとも解釈できる。

構成（続き）

第26条 トラフィックデータの**迅速な**保全および部分開示［暫定的合意］

第27条 証拠開示命令［暫定的合意］

第28条 保存された電子データ stored electronic data の捜索および押収［暫定的合意］

第29条 トラフィックデータのリアルタイム収集［暫定的合意］

第30条 コンテンツデータの傍受［暫定的合意］

最も問題が多いとおもわれるコンテンツの盗聴捜査

第31条 犯罪収益の凍結、押収及び没収［暫定的合意］

第32条 犯罪記録の設定［暫定的合意］

第33条 証人の保護［暫定的合意］

第34条 被害者に対する支援と保護［暫定的合意］

第五章 国際協力

他国によるスパイ活動に自国政府が加担して私たちのコミュニケーションを監視する体制が構築されかねない

第35条 国際協力の一般原則

第36条 個人データの保護［暫定的合意］

第37条 引渡し［暫定的合意］

第38条 受刑者の移送［暫定的合意］

第39条 刑事手続の移管［暫定的合意］

第40条 法的相互援助に関する一般原則及び手続

最終草案の内容

構成（続き）

第41条 年中無休のネットワーク

第42条 保全された電子データの**迅速な**保存を目的とする国際協力

第43条 保全されたトラフィックデータの**迅速な**開示を目的とする国際協力

第44条 保存された電子データへのアクセスにおける法的相互援助［暫定的合意］

第45条 トラフィックデータのリアルタイム収集における法的相互援助［暫定的合意］

第46条 コンテンツデータの傍受における法的相互援助 ［暫定的合意］

国境を越えた盗聴捜査が制度化されることになる

第47条 法執行協力［暫定的合意］

第48条 共同捜査［暫定的合意］

第49条 没収における国際協力による財産の回復のためのメカニズ［暫定的合意］

第50条 没収を目的とする国際協力［暫定的合意］

第51条 特別協力［暫定的合意］

第52条 没収された犯罪収益又は財産の返還及び処分［暫定的合意］

第六章 予防措置

第53条 予防措置

最終草案の内容

構成（続き）

第七章 技術援助及び情報交換

第54条 技術援助及び能力開発

第55条 情報交換［暫定的合意］

第八章 実施の機構

第57条 この条約の締約国会議

第58条 事務局［暫定的合意］

第九章 最終規定

第59条 条約の実施［暫定的合意］

第61条 議定書との関係［暫定的合意］

第62条附属議定書の採択

第63条 紛争の解決［暫定的合意］

第64条 署名、批准、受諾、承認及び加入［暫定的合意］

第66条 改正

第67条 破棄［暫定的合意］

先進国などによる国策としての途上国への監視技術の輸出競争を後押しすることになる。

条約の論点

- 前文

「情報通信テクノロジー・システムを使用することは、人身売買、移民の密入国、銃器、その部品、構成部品、弾薬の不正製造および取引、麻薬取引、文化財の取引など、テロリズムおよび国際組織犯罪に関連する犯罪を含む刑法犯罪の規模、速度、範囲に多大な影響を及ぼしうることを懸念」

「国家間の協調と協力を強化し、国内法制と枠組みを改善し、予防、摘発、捜査、訴追を含むあらゆる形態のサイバー犯罪に対処する国家当局の能力を高める必要性」

- 条約の目的 (1 条)

サイバー犯罪をより効率的かつ効果的に防止し、及びこれと闘うための措置を促進し及び強化すること。[暫定的合意]。

サイバー犯罪の防止及び対処に関する国際協力

特に開発途上国の利益のために、サイバー犯罪を防止、技術支援、能力構築

- どのような犯罪を対象にするのか

「締約国は、自国が締約国である他の適用可能な国際連合条約及び議定書を実施するに当たり、情報通信技術システムを使用して行われる犯罪については、当該条約及び議定書に従って定められた刑法犯罪も国内法上の犯罪とみなされることを確保する。」

条約の論点

第23条．手続き上の措置の範囲

各締約国は、特定の犯罪捜査又は手続のためにこの章に定める権限及び手続を定めるために必要な立法その他の措置を採用するものとする。

この条約に別段の定めがある場合を除くほか、各締約国は、この条第一項にいう権限及び手続を次の各号に適用する。

(1)この条約に従って定められた刑法犯罪

(2)情報通信テクノロジー・システムを利用して行われたその他の刑法犯罪。

(3)あらゆる刑法犯罪の証拠を電子形式で収集すること。

各国は、この条約で定めている犯罪捜査の手続きや権限について、この条約が明記している犯罪(7条から21条)だけでなく、情報通信テクノロジーを用いた犯罪であれば、適用でき、また、電子的なデータを証拠そして収集可能としている。事実上歯止めなく、捜査機関の権限が強化され、しかも、国際法の越境性を悪用して、各国捜査機関が国境を越えた包囲網形成が容易になるような構造になっている。この点は、特に、自国政府から迫害されて国外に逃れている難民やジャーナリスト、人権活動家、反政府運動活動家に深刻な打撃を与えることになる。

条約の論点

- 第４章 手続き上の措置および法の執行

  各締約国は、特定の犯罪捜査又は手続のためにこの章に定める権限及び手続を定めるために必要な立法その他の措置を採用するものとする。

- 第28条． 保存された電子データ stored electronic data の捜索および押収［暫定的合意］

  1． 各締約国は、当該締約国の領域内において、 以下について、所管当局に捜索し又はこれと同等の方法でアクセスする権限を与えるために必要とされる立法措置及びその他の措置を採用するものとする

  (a) 情報通信テクノロジー・システム、その一部及びそこに保存されている電子データ。

  (b) 捜索対象の電子データが記憶されている電子データ記憶媒体

  2. 各締約国は、自国の当局 authorities が本条第１項 (a) に従って特定の情報通信テクノロジー・システム又はその一部を捜索し又はこれと同等の方法でアクセスする場合において、求められた電子データが自国の領域内の他の情報通信テクノロジー・システム又はその一部に保存されており、かつ、当該データが最初のシステムから適法にアクセス可能であるか又は最初のシステムで利用可能であると信じるに足りる根拠があるときは、当該当局は、当該他の情報通信テクノロジー・システムへのアクセスを得るための捜索を迅速に行うことができることを確保するために必要とされる立法措置その他の措置を採用するものとする。

条約の論点

- 第28条． 保存された電子データ stored electronic data の捜索および押収［暫定的合意］
  - 裁判所による令状発付を義務づけていない
  - 捜索対象のシステムからネットワークを介してアクセスできる他の場所にあるシステムにも捜索対象を拡大して構わない
  - 捜索対象のシステムに精通している個人に命令して捜査に協力させる

  捜査機関に権限を与えるように国内法を変えることを義務づけている
- リアルタイムでの傍受

  29条 トラフィックデータの傍受

  30条 コンテンツの傍受

条約の論点

- 30条 コンテンツデータの傍受［暫定的合意］

各締約国は、国内法によって定められた重大な刑法犯罪の範囲に関し、情報通信テクノロジー・システムにより送信される自国の領域内の特定通信のコンテンツ・データをリアルタイムで収集することについて、その所管当局に次のことを行う権限を付与するために必要な立法措置及びその他の措置を採用するものとする：

(a) 当該締約国の領域内において、技術的手段の適用を通じて、収集し、又は記録すること。

(b) サービスプロバイダーに対し、その既存の技術的能力の範囲内で、次のことを義務付ける：

(i) 当該締約国の領域内において、技術的手段の適用を通じて、収集し、又は記録すること。

(ii) 所管当局に対し収集又は記録について協力し、かつ、これを支援すること。

2. 締約国が、その国内法体系の原則により、この条の第一項（ａ）にいう措置を採用することができない場合には、その代わりに、その領域における技術的手段の適用を通じて、その領域における特定通信のコンテンツデータのリアルタイムの収集又は記録を確保するために必要とされる立法上の措置その他の措置を採用することができる。

条約の論点

リアルタイム傍受についての本条約の基本的な性格は、

- 警察などが裁判所の令状なしで迅速に捜査できる権限を持つ
- ほぼ全ての犯罪について、リアルタイムでの盗聴捜査ができるような立法措置を採用する
- サービスプロバイダーに対し、警察などへの協力を義務づける立法措置をとる
- これらの措置が現行法ではできない場合は、特定通信のコンテンツデータのリアルタイムの収集又は記録を確保するために必要とされる立法上の措置その他の措置を採用することを求める

現行法で対応できない場合は、本条約に合わせた形での国内法の改悪が義務とされる。

条約の論点

国際的な法的相互援助

第 40 条． 法的相互援助に関する一般原則及び手続

締約国は、この条約に従って定めるものの犯罪に関する捜査、訴追及び司法手続並びにこの条約に従って定める犯罪及び重大犯罪に関する電子的形式による証拠の収集の目的のために、相互に最も広範な相互法的援助を与える。

#人権よりも捜査機関の利益を優先させる可能性が高い

協力の内容には以下が含まれる

- 情報通信テクノロジー・システムの手段により保存された電子データを捜索し、又はこれに類似の方法でアクセスし、差し押さえ、又はこれに類似の方法で確保し、及び開示すること
- トラフィックデータをリアルタイムで収集すること；
- コンテンツデータを傍受すること

国内法に定める条件及び手続に基くとされているが、条約の趣旨を汲んで国内法が改悪される可能性が高い

条約の論点

捜査機関への協力の事実上の義務化 (53 条)

法執行機関又は検察官と、非政府組織、市民社会組織、学術機関及び民間団体のような公的部門以外の関連する個人及び団体との間の協力を強化

サービス・プロバイダーに対し、当該サービス・プロバイダーの製品、サービス及びカスタマーのセキュリティを強化するために、国内事情に照らして実行可能な場合には、かつ、国内法によって認められる限度において、効果的な措置をとるよう奨励する

締約国は、必要な限度において、国際機関及び地域機関並びに関連する二国間及び多国間の協定又は取極の枠組みにおける技術援助及び能力構築の効果を最大化するための努力を強化するものとする。[暫定的合意]。

締約国は、技術支援プログラム及び能力構築プロジェクトを通じ、途上国がこの条約を実施するための努力に財政的に貢献することを目的とする自発的なメカニズムを定めることを検討するものとする。[暫定的合意]。

経済援助の監視社会化や自国の監視技術資本の途上国におけるビジネスチャンスを政府や国連が後押しすることになる

条約への様々な批判 (1)

この条約はサイバー犯罪の定義が極めて緩く、しかもその緩さは意図的なものである。中国やロシアのような権威主義国家（その代表団がこの条約の推進力となっている）では、「サイバー犯罪」とは、コンピューターを使って行うものであれば、「政府が嫌うものは何でも」という意味になっている。「サイバー犯罪」とは、オンライン上での政府批判、宗教的信念の表明、LGBTQの権利を支持する資料などを意味する。

サイバー犯罪条約に署名した国は、他国の「サイバー犯罪」（その定義がどうであれ）と闘うために協力する義務を負う。例えば、彼らは自国内のオンラインサービスにユーザーの個人データを提供するよう強制したり、継続的な監視のためにシステムにバックドアを設置するよう従業員に圧力をかけたりすることで、監視データを提供することが求められる。

あなたの政府はあなたやあなたの愛する人々をスパイするよう要請されるかもしれないし、ハイテク企業の従業員にあなたのアカウントやデバイスをバックドアするよう命令されるかもしれない。

(doctorow.medium.com)コーリー・ドクトロウ 国連サイバー犯罪条約は悪夢だ

条約への様々な批判 (2)

サイバー犯罪を ICT が関与するあらゆる犯罪と同一視しており、各国政府はこれを利用して、サイバー犯罪の定義を拡大した国内法を成立させることを正当化する可能性があります。

私たちは、第 3 条を、第 7 条から第 17 条に基づいて定められた違反行為についての特定の犯罪捜査と訴追に限定することを提言します。捜査と協力の権限が第 7 条から第 17 条を超えて拡張されるのであれば、第 23 条と第 35 条は、重大な犯罪が行われたと信じるに足る合理的な疑いがあり、その犯罪が国際人権法の下で法的に犯罪とされる特定のケースに限定されるべき

子どもの性的虐待の資料に対する条約のアプローチは、子どもの権利を侵害する危険性があります。第 14 条 4 項は、国連子どもの権利委員会の指針に反して、同じような年齢の子ども同士の同意に基づく行為を犯罪化するものです。第 14 条 2 項は、証拠としての価値、科学的な価値、芸術的な価値を持つ資料を犯罪化する危険性があり、子どもの権利侵害を調査する人権団体の活動を危険にさらすものです。

EFFおよびヒューマン・ライツ・ウォッチの国連サイバー犯罪条約に関する声明 (範囲、人権保障措置、子どもの権利に関して)

条約批判 (3)

もしあなたがＡ国の活動家で、Ｂ国の人権侵害についてツイートしており、政府高官や国王を批判することが、曖昧なままのサイバー犯罪法の下で、両国で重大な犯罪とみなされた場合、国連サイバー犯罪条約は、Ａ国がＢ国のためにあなたをスパイすることを認める可能性がある。これは、Ａ国が司法当局の事前承認なしにあなたの電子メールにアクセスしたり、あなたの居場所を追跡したりすることができ、たとえそれがもはや捜査に影響しなくなっても、この情報を秘密にしておくことができることを意味する。

政府を批判することは、フィッシング攻撃を仕掛けたり、データ漏洩を引き起こしたりすることとはかけ離れている。しかし、これはコンピューターを使用することであり、国内法で定義された重大犯罪であるため、現在記されている通り、この条約の国境を越えた政府によるスパイ活動の範囲に含まれる。

これは誇張ではない。ロシアや中国のような国々では、重大な「サイバー犯罪」は、コンピューターに関わることであれば政府が認めないあらゆる活動の総称となっている。この広範で曖昧な重大犯罪の定義によって、これらの政府はサイバー犯罪の取締りを装って政治的反体制派を標的にし、言論の自由を抑圧することができる。

LGBTQ+ の権利を非合法化している国では、ソーシャルメディアに虹の旗を投稿することが重大なサイバー犯罪とみなされる可能性がある。人権侵害に関するリークデータに基づいて記事を発表するジャーナリストや、ソーシャルメディアを通じて抗議活動を組織するデジタル活動家は、条約草案の下ではサイバー犯罪を犯したと非難される可能性がある。

(EFF)広範な適用範囲は、表現行為に対する国境を越えたスパイ行為を容認する： 国連サイバー犯罪条約草案に反対すべき理由

条約批判（4）

OHCHR は、多くの条項が国際人権基準を満たしていないという重大な欠点に依然として懸念を抱いている。これらの欠点は、表現の自由を不当に制限し、反対意見を標的にし、通信のプライバシーと匿名性を恣意的に妨害するために、一部の司法管轄区において既存のサイバー犯罪法がすでに拡大的に使用されていることを背景として、特に問題となる。

OHCHR はこの制度における犯罪化の範囲を狭くし、サイバーに依存する犯罪に限定するよう勧告してきた。これらの犯罪とは、データやシステムの完全性、機密性、可用性に対する犯罪、これらの犯罪を犯す目的でデバイスを悪用する犯罪、コンピュータ詐欺など限られた特定のコンピュータ関連犯罪など、コンピュータデータやシステムに本質的に関連する犯罪である。先に述べたように、サイバー犯罪の定義が広すぎる法律は、国際人権法で保護されているオンラインコンテンツに関連する行為を犯罪化するなど、表現の自由に対する権利に不当な制限を課すために頻繁に使用される。特に、曖昧で漠然とした文言や広範な犯罪の定式化によって、狭い範囲を超えて拡大することは、将来の人権侵害や濫用のリスクを大いに高めることになる。

国際連合人権高等弁務官事務所 (OHCHR)5 月に発表されたサイバー犯罪条約草案の第 3 次改訂版に対しするコメント

私たちは何をすべきか

- サイバー犯罪条約に明確に反対する意思表示が必要
  - 日本政府が条約に反対することを働きかける
- もし総会で条約草案が採択された場合
  - 日本は批准すべきではない
  - 日本の国内法の改正などが必要になる
- 改憲との連動（通信の秘密、表現の自由など）、サイバー安全保障関連の法整備、移民難民の人権問題などへの影響についても関心を持つ必要がある